

Communication Vulnerabilities and Mitigations in Wind Power Supervisory Control and Data Acquisition Systems

Bill Young

Secure Networks & Information Systems

Sandia National Laboratories

Telephone: (505) 844-8327

E-mail: wfyoung@sandia.gov

Mark Rumsey

Wind Energy Technology Department

Sandia National Laboratories

Telephone: (505) 844-3910

E-mail: marumse@sandia.gov



Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States
Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.





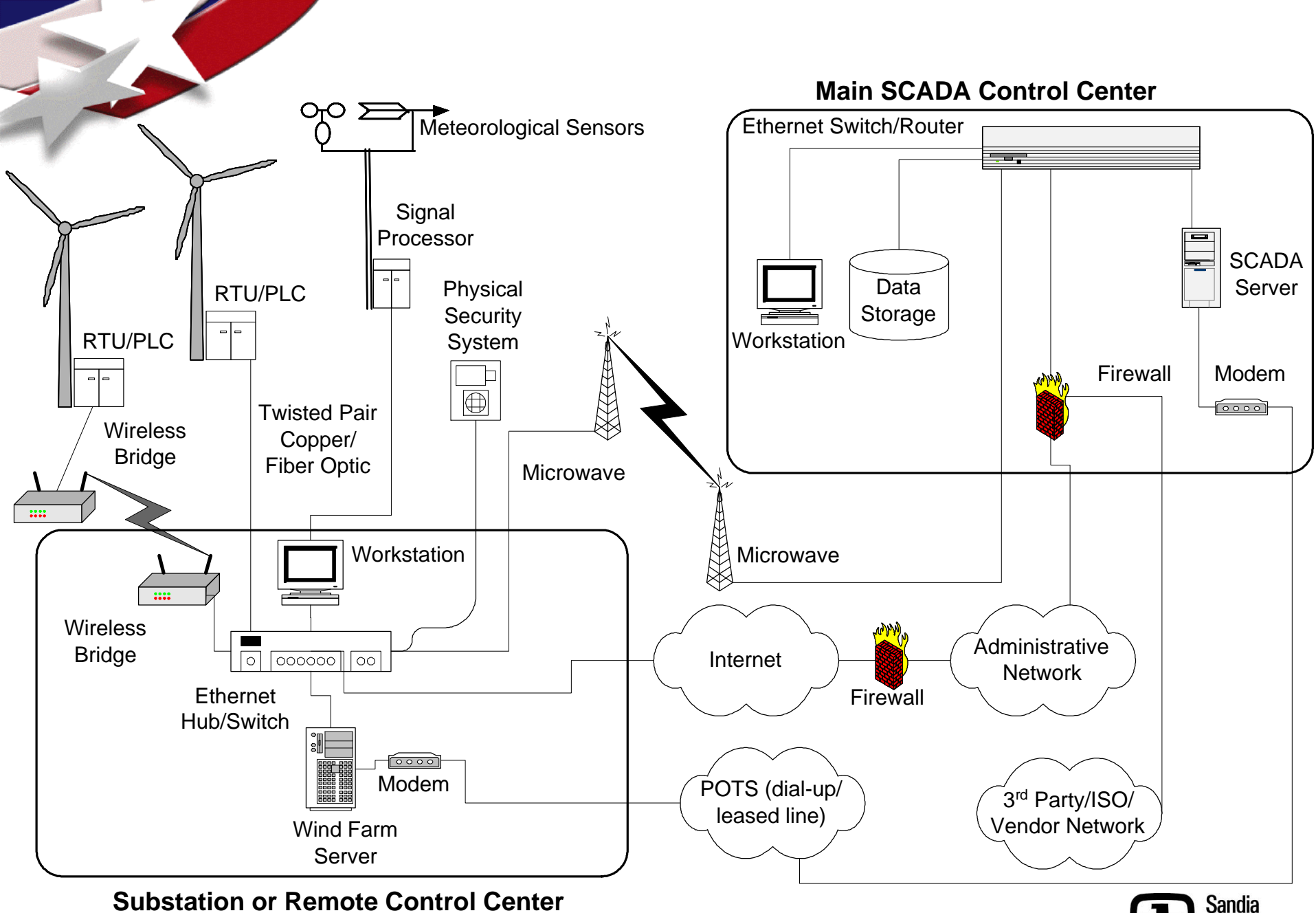
Presentation Outline


- **Elements of Supervisory Control and Data Acquisition (SCADA) Security**
- **Example Wind Power SCADA System**
- **Number One Vulnerability**
- **Interface to Other Networks**
- **Bridged Wireless Communications**
- **Conclusion**



Security Requires an Effective Combination of:

- **Awareness**
- **Administration**
 - **Policy**
 - **Procedures**
 - **Training**
- **System Implementation**
 - **Technology**
 - **Device Configuration**





Trends in Technology for Wind Power SCADA Systems

- **Modern technology**
 - Standard Operating Systems
 - Windows, Unix, Linux
 - Standard networking
 - Ethernet, TCP/IP
 - Wireless connectivity
 - IEEE 802.11, Bluetooth™
- **Distributed data warehousing**
- **Internet availability of data and control**
- **3rd Party/Vendor/ISO network connections**
- **Intelligent field devices**
- **Variety of data types on the SCADA network**
 - SCADA monitor, SCADA control, SCADA historical, maintenance, prototype testing, network administration, engineering, and non-SCADA data for physical security monitoring



Highest Priority Vulnerability: The SCADA system has no specific documented security policy or security plan.

Solution:

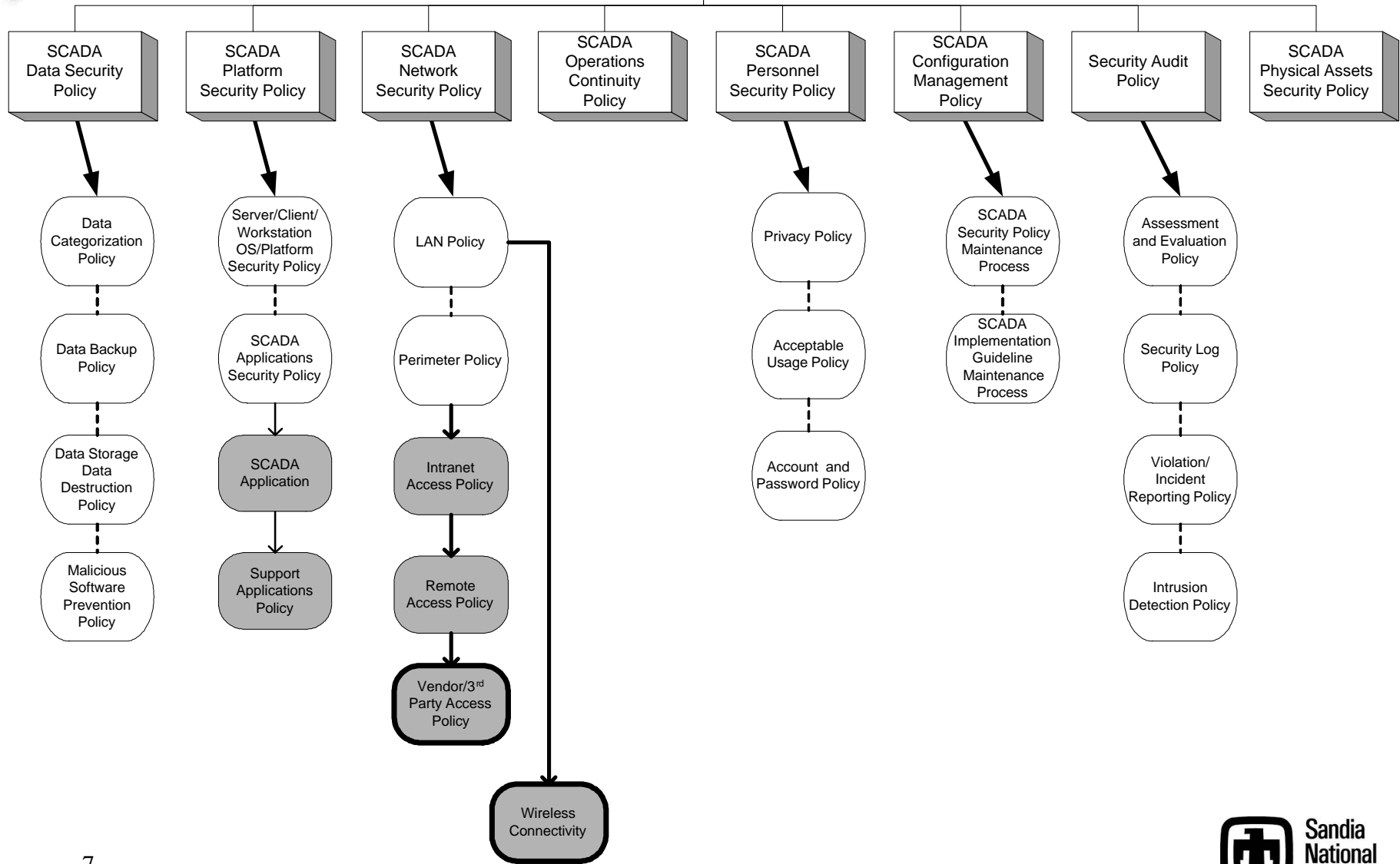
SCADA System Security Policy

SCADA Security Policy Framework™

- **Policies, Standards, and Procedures**
- **Assignment of Security Responsibilities**
- **Effective Use of Protective Technology**
- **Security Education and Training**
- **Risk Management**
- **Contingency Planning**
- **Security Accreditation of SCADA systems**



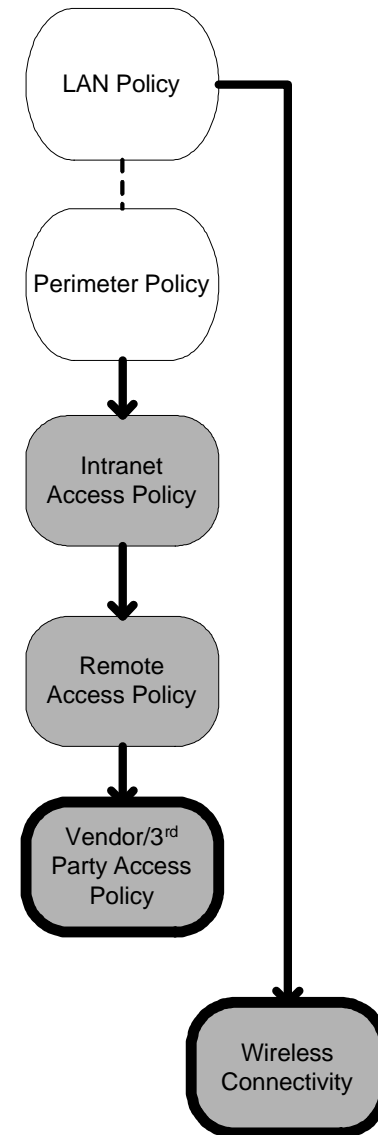
SCADA System Security Policy
SCADA Security Policy Framework™



Network Security Policy

SCADA Security Policy Framework™

- **Network Security Policy** represents one category of the overall SCADA Security Policy (previous slide)
- **Grayed rounded rectangles depict supporting or lower-level elements of the Network Security Policy**
- **LAN Policy** covers the use of wireless technology within the SCADA network
- **Perimeter Policy** Addresses Vendor/3rd Party/ISO access to the SCADA network

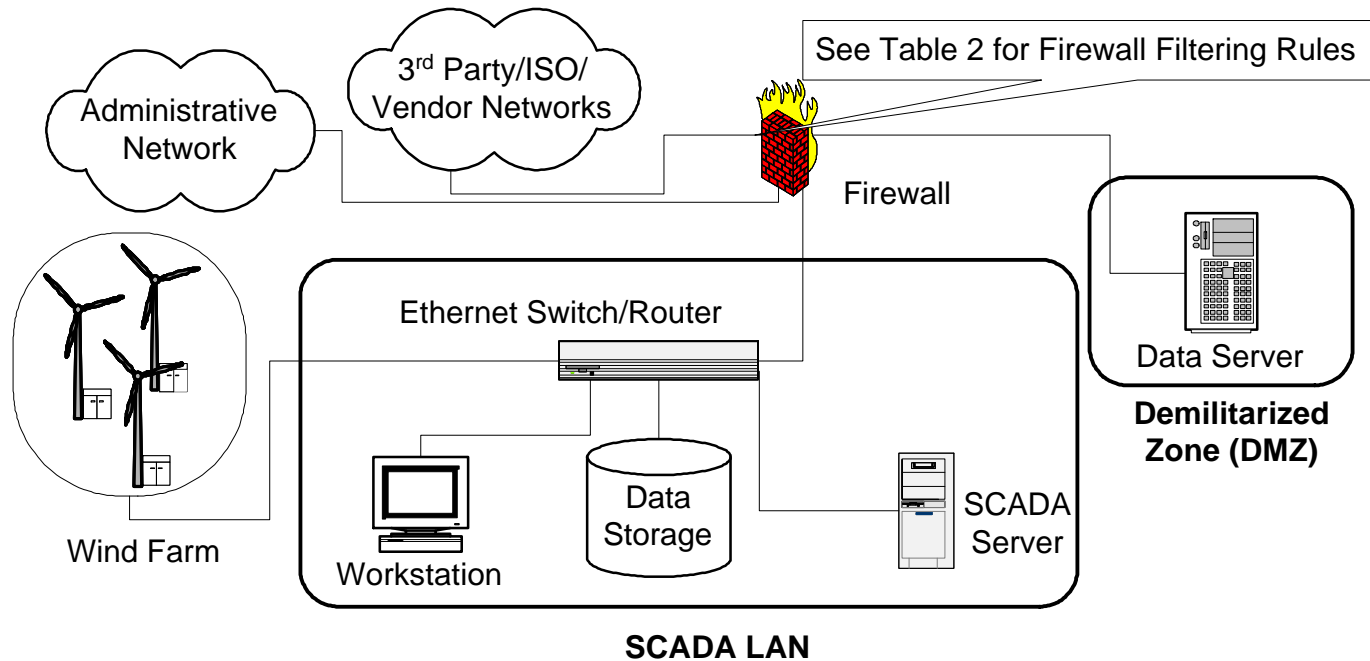




Interfacing to 3rd Party/Vendor/ISO and Administrative Networks

- **Internet connectivity**
 - Utilities connect their SCADA system to their enterprise network, which in turn is connected to the Internet (or remote access) so that public data may be made available easily, and with low latency.
 - **Problem:** *logical connectivity for any attacker worldwide*
- **Security perimeter**
 - Perimeter firewalls often not adequately configured, if they exist at all.
 - Remote access and network back doors (connections to contractors, partners, and others) are often not adequately protected.
 - **Problem:** *attackers can successfully penetrate the SCADA network*
- **Vendors**
 - Remote access to vendors often part of software maintenance process
 - **Problem:** *access can expose the SCADA network to vulnerabilities on the vendor's network*

Connections to Other Networks Via a DMZ



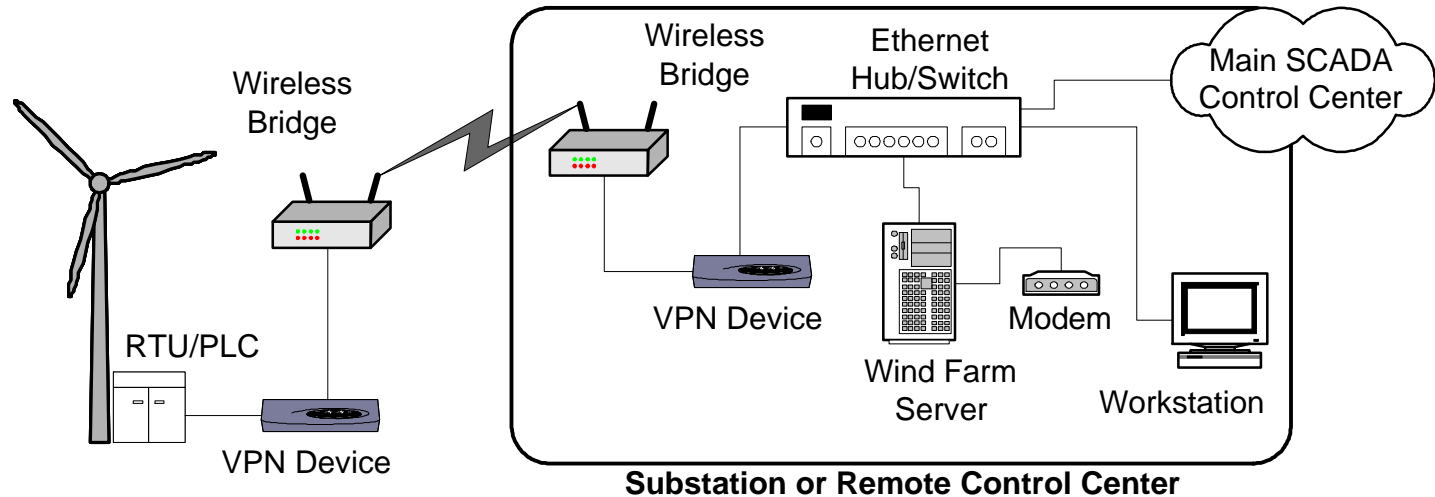
- **Connection utilizes an intermediate platform for data transfer**
- **Firewall restricts the connectivity allowed between network segments**
 - No direct connectivity is allowed between 3rd Party/ISO/Vendor or Administrative Networks and the SCADA LAN
- **Firewall is physically and logically secured**
 - Managed by the SCADA network administrators
 - Unnecessary services on the firewall such as telnet, FTP, HTTP, disabled during normal operations



Bridged Wireless Communications

- **Security perimeter**
 - Wireless medium, i.e. the air, cannot be physically secured
 - Antennae interface is actually a boundary of the SCADA network
 - **Problem:** *attackers have access the SCADA network communication medium*
- **Wireless Communications**
 - Wireless channel access control messages and processes are not adequately protected
 - **Problem:** *attackers can introduce invalid wireless channel control messages or potentially access the SCADA network*
- **Wireless Channel**
 - Data protection mechanisms are ineffective or non-existent
 - **Problem:** *attackers can capture or alter sensitive SCADA data*

Wireless Bridge Network with VPN Devices



- **The Security Policy mandates the level of security for the wireless link**
 - Strong encryption, authentication, integrity
- **VPN technology provides protection of application data between VPN devices**
 - Does not protect device management data between wireless bridges
- **VPN and Wireless bridge devices physically and logically secured**
 - Unnecessary services on the devices disabled
 - Physical protection prevents unauthorized reconfiguration of devices



Conclusion: Robust Security Requires an Effective Combination of Security

- **Awareness**
- **Administration**
 - Policy
 - Procedures
 - Training
- **System Implementation**
 - Technology
 - Device Configuration